Schrödinger's Crisis: Building and examining an ecosystem of EU Product Cybersecurity

1 Introduction

Standardisation – a term that invites a diversity of opinion, but seldom a doubt on its criticality to modern markets.[1] Yet, as an area of research, it has been characterised as under-investigated, especially from an interdisciplinary lens.[2] A prevalent form of trans-national rule making, standardisation has been an important part of European regulation as well, fostering the formation of an internal market by bolstering technical harmonisation across EU Member States.[3]

1.1 European Standardisation: A brief evolutionary overview.

The functioning of European standardisation activity has evolved over the past few decades. Starting as a framework comprising multitudes of technically detailed Directives and riddled with legitimacy and consensus-building problems, a major attempt at streamlining it arrived in the 'New Approach' of 1985.[4] The New Approach entailed limiting Directives to specifying essential requirements, geared towards protection of public interests such as health and safety, while technical detail would be added through 'harmonised standards', essentially voluntary avenues of compliance developed by the European Standardisation Associations (ESOs).[5]

Though further strengthened and legitimised through judicial action, becoming a *de facto* part of EU law[6] with accompanying market effects strongly incentivising their uptake despite their voluntary nature,[7] questions about the applicability of EU free movement provisions to products complying with privately developed standards remained subject to judicial discussion.[8] The adoption of the Regulation on European Standardisation (Standardisation

---

[1] "Standards are acknowledged to be the building blocks for the information society" in Werle, R. & Iversen, E. J., Promoting Legitimacy in Technical Standardization, (2006) Science, Technology & Innovation Studies 2 (March 2006), pp. 19-39, at 20;
"…technical standards exist in virtually every sector… and are crucial for the adoption and diffusion of new technologies" in Kanevskaia, O., Delimatsis, P., & Bijlmakers, S., The European telecommunications Standards Institute (ETSI): in search for legitimacy and resilience of European standardization, (2024) Innovation: The European Journal of Social Science Research 37:5, https://doi.org/10.1080/13511610.2024.2395262, p. 1269;
"Researchers in these disciplines [contributing to standardisation] have very diverse views regarding necessary future [standardisation] research priorities" in De Vries, H. *et al,* Standardization: Towards an agenda for research, (2018) International Journal of Standardization Research 16:1 (de Vries *et al* 2018), DOI: 10.4018/IJSR.2018010104, p. 52

[2] De Vries *et al* 2018 (N1), p. 56

[3] Kanevskaia, O., The law and practice of global ICT standardization, (2020) Tilburg University (Kanevskaia 2020), https://research.tilburguniversity.edu/en/publications/471246d9-e0d7-4722-ab72-c81a64a4428c, p. 61

[4] Kanevskaia 2020 (N3), p. 61

[5] Council Resolution of 7 May 1985 on a New Approach to technical harmonization and standards, OJ C 136/1 (New Approach Resolution), https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:31985Y0604(01)

[6] Case C-120/78, Rewe-Zentral AG v Bundesmonopolverwalting fur Branntwein, (1979) ECR 1979-00649

[7] Schepel, H., The New Approach to the New Approach: The Juridification of Harmonized Standards in EU Law, (2013) Maastricht Journal of European and Comparative Law 20:4 (Schepel 2013), https://doi.org/10.1177/1023263X1302000404, p. 528;

[8] Case C-227/06, Commission v Belgium (2008) ECR 2008-I-00046; Case C-185/08, Latchways PLC & Eurosafe Solutions BV v Kedge Safety Systems BV & Consolidated Nederland BV, ECR 2010-I-09983; Case

Regulation)[9] provided some legislative clarity by further formalising the process of developing harmonised standards shortly followed by the landmark *James Elliott* case qualifying Harmonised Standards as part of EU law as they are developed as measures to apply law.[10] However, another issue in European Standardisation gained prominence. In a market majorly occupied by services, standards for services were extremely lacking,[11] prompting a call for increased standardisation of services.[12]

1.2 Standards and Cybersecurity – A timely alliance of European policy priorities.

These last developments were occurring parallel to cybersecurity of European goods and services was becoming a priority in European policy; a recognition that the market was becoming increasingly dependent on digital technologies.[13] Information and Communication technology was rapidly becoming the foundation upon which good and services are offered. Cybersecurity started being recognised as another aspect of public interest, and soon policy proposals prioritised making European goods and services cybersecure.[14] These policy proposals found legislative actualisation through the NIS2 Directive – a rework of the older NIS Directive, and the EU Cyber-Resilience Act (CRA).[15] The former prescribes high-level operational cybersecurity obligations to be performed by market operators providing services in the Union, implemented and enforced through Member State transposition. The latter functionally harmonises throughout the EU minimum cybersecurity requirements[16] that must be met by "digitally enabled products" (PDEs)[17] to access the European market, with additional mechanisms for conformity assessment and continuity.[18] Both legislations have an immense scope; the NIS2 Directive applies to most market operators, especially those rendering services critical to the Union economy and the CRA applies to all PDEs being brought into the Union market.

Both legislations also acknowledge compliance with technical standards as an avenue for demonstrably conforming services and products respectively.[19] However, only the CRA

C-171/11, Fra.bo SpA v Deutsche Vereiniging des Gas-und Wasserfaches eV (DVGW), (2012) ECLI:EU:C:2012:453

[9] Regulation (EU) No 1025/2012 on European Standardisation, OJ L 316/12 (Standardisation Regulation), The Regulation defined harmonised standards as standards developed or adopted by ESOs in response to standardisation requests made by the European Commission in support of relevant EU law (Article 2(1)(c)). It also further formalised the process of developing such standards.

[10] Case C-613/14, James Elliott Construction Limited v. Irish Asphalt Ltd. (2016) ECLI:EU:C:2016:821

[11] Vallejo, R., The Private Administrative Law of Technical Standardization, (2021) Yearbook of European Law 40:1 (Vallejo 2021), https://doi.org/10.1093/yel/yeab011 p. 173

[12] The Standardisation Package: European Standards for the 21st Century, COM (2016) 358 final, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52016DC0358

[13] Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace, JOIN (2013) 1 final

[14] The EU's Cybersecurity Strategy for the Digital Decade, JOIN (2020) 18 final (Cybersecurity Strategy 2020), https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52016DC0358, Section 1

[15] Directive (EU) 2022/2555 on measures for a high common level of cybersecurity across the Union, OJ L 333/80 (NIS2 Directive), https://eur-lex.europa.eu/eli/dir/2022/2555/2022-12-27/eng; Regulation (EU) 2024/2847 on horizontal cybersecurity requirements for products with digital elements, OJ L 2024/2847 (Cyber Resilience Act), https://eur-lex.europa.eu/eli/reg/2024/2847/oj/eng

[16] Cyber Resilience Act (N15), Annex I

[17] Cyber Resilience Act (N15), Article 3(1)

[18] Cyber Resilience Act (N15), Chapters III & IV

[19] NIS2 Directive (N15), Articles 24 & 25; Cyber Resilience Act (N15), Articles 27 & 32

pursues the Harmonised Standards route, enabling direct employment of the Standardisation Regulation framework for PDEs but not for services subject to NIS2 obligations. Nevertheless, both legislations exhibiting significant reliance on technical standards for their implementation does lend credence to the view that technical standards, especially Harmonised Standards – essentially a form of private rule-making – might *de facto* be evolving into a major part of public rulemaking in the EU cybersecurity governance realm.[20]

The impacts and implications of this evolution have not gone unnoticed. For example, the Court of Justice of the European Union (CJEU) recently ruled on accountability for, and legitimacy of standards thusly adopted, ruling that disclosure and access to such harmonized standards is a matter of public interest that would override commercial interests of parties involved in the standardization process.[21] The prevalence of standards in Union regulation has been examined from various angles, including *inter alia* constitutional perspectives[22] and market perspectives.[23] In that vein, this article investigates standardisation trends from the standpoint of European cybersecurity governance.

1.3 Aims, contributions and limitations of this article.

Contemporary standardisation literature observes legislative dependence on standards from diverse viewpoints, including deconstructions of their commercial value vis-à-vis market needs for legal certainty,[24] supply chain impacts, conformity assessment questions,[25] and their ability to affect dynamics among actors in a particular regulatory aegis.[26] This article focuses on the effect of standards on actor dynamics in the European cybersecurity space, inspired by questions arising from the aforementioned broad-scoped cybersecurity legislations;[27] questions specifically relating to the balance of rule-making power among these actors.

---

[20] Veale, M., and Borgesius F. Z., Demystifying the draft EU Artificial Intelligence Act, (2021) Computer Law Review International, 22(4), 97-112 (Veale and Borgesius 2021), available at https://doi.org/10.9785/cri-2021-220402; Fra.bo Case (N8); Schepel 2013 (N 7), 528; Ajmera, P., Cybersecurity in the Internet of Things: Trends and Challenges in a Nascent Field, (2025) Computer Law and Security Review 59/106204, https://doi.org/10.1016/j.clsr.2025.106204, Sections 4.2-4.3

[21] Judgement of the Court of Justice of The European Union (CJEU) (Grand Chamber) in Case C-588/21 of the CJEU, Public.Resource.Org Inc. & Anr. v The European Commission and Ors. (Malamud Case), Paragraphs 83-85 and 89

[22] For example, a constitutional view on the Malamud case (N26) is presented in Kanevskaia, O., *Is it really all about the money? The future of European standardization after* PublicResourceOrg*,* (2025) European Journal of Risk Regulation 16, 344-51 (Kanevskaia 2025), available at doi:10.1017/err.2024.64

[23] For example, the use of standards and their prevalence in economic crises have been explored in Delimatsis, P., Kanevskaia, O., and Verghese, Z., *Strategic Behavior in Standards Development Organizations in times of Crisis*, Texas Intellectual Property Law Journal, 29(2), 127-185 (Delimatsis and Ors., 2021) and Delimatsis, P., *Transnational Economic Activism and Private Regulatory Power*, (2023) Journal of International Economic Law 26, 559-76 (Delimatsis 2023), available at https://doi.org/10.1093/jiel/jgad028

[24] Kanevskaia 2025 (N22)

[25] de Vries, H., *et al, Standardization: Towards an Agenda for research,* (2018) International Journal of Standardization Research 16-1, (de Vries *et al* 2018), available at https://www.igi-global.com/gateway/article/full-text-pdf/218521

[26] Delimatsis 2023 (N23)

[27] *Supra* Note 15

In attempting to make this determination, this article proposes employing an 'ecosystems theory'[28] based view for two reasons. First, it enables a holistic view of the European cybersecurity space not just as a group of static actors, but as a group of otherwise independent actors dynamically interacting through factors that drive alignment among them. Second, the framework established by the Standardisation Regulation is unique in its attempt to balance commercial interests, public interests and consumer protection in a manner consistent with constitutional principles like transparency, accountability and legitimacy.[29]

These reasons also bring with them some limitations. The unique nature of the Standardisation Regulation framework (hereinafter "the HES framework") causes this research to limit its focus to Harmonised European Standards (HESs), i.e., standards developed by ESOs pursuant to requests by the Commission. Thus, the current attempt at building an ecosystems theory-based view must limit itself solely to standardisation activity supporting the CRA, i.e., HESs for PDE cybersecurity. While constructing such a view for standards supporting the NIS2 Directive does seem possible, such a construction would require preceding analysis associating characteristics unique to HESs to NIS2 relevant standards which *prima facie* do not exhibit those characteristics. The preceding analysis, and therefore an NIS2 based construction is unfortunately outside the scope of the current article.

Secondly, the novelty of the CRA as a legislative instrument, having only been published in October 2024, means that several aspects of the legislation and supporting HESs have not been put into practice yet. While this does not prevent a theoretical analysis, the analysis does point to some trends and possible impacts. These findings are grounded in theoretical application and stem from comprehensive legal reasoning, but in the absence of measurable practice-based activity remain theoretical constructs.

This article is structured as follows. Section 2 examines contemporary theoretical perspectives on governance of multi-actor regulatory spaces, assessing the benefits and drawbacks of applying them to European PDE cybersecurity and simultaneously arguing in favour of an ecosystems-based approach. Section 3 identifies and elaborates on the elements required to build an ecosystems-based view on European PDE cybersecurity. Section 4 completes the construction of this ecosystems-based view and examines trends and possible impacts of the resultant dynamic shifts among actors in that space. Concluding remarks following this synthesis the articles findings and solidify the perspectives arrived at.

Section 2: Towards an ecosystem of EU Product Cybersecurity: Theoretical perspectives

The need for an ecosystems-based perspective is guided primarily by observations of market operations, and an increasing prevalence of ecosystems-based analyses in business and strategy

---

[28] Jacobides, M. Cennamo, C., Gawer, A., *Towards a theory of ecosystems*, (2018) Strategic Management Journal 39, 2255-76, available at doi:10.1002/smj.2904 (Jacobides & ors 2018),

[29] Delimatsis, P., A shared regulatory space to advance the EU Internal Market: The Evolution of the European Standardisation System, in Delimatsis, P., & Monti, G., (eds.), EU Law and Regulatory Spaces: Essays in Honour of Leigh Hancher, (2026) Hart Publishing (Delimatsis 2026), DOI: 10.5040/9781509991914.ch-002, p. 39-41

literature.[30] The word 'ecosystem' itself has covered quite an interesting journey, originating primarily in biological contexts, slowly being co-opted in industrial (primarily technological) circles, to being prominent now in market and industry related literature; with literature being examined to coalesce the concept into categories based on how actors and institutions organise themselves.[31] In this context, how the HES framework guides such institutional organisation becomes pertinent.

2.1 From 'systems' to 'ecosystems': Accounting for non-linear institutional interaction

Theoretical perspectives on product regulations and governance have evolved over time. Privatisation of traditionally public capacities and the evolution of a globalised supply chain have led to the development of 'institutional' theories of regulation that view the regulatory balancing of interests from an institutional lens rather than a strictly public or private actor-led lens.[32] These institutional perspectives find impetus in recognition of the reliance on transnational private regulation posing a challenge to the fundamental notion of which interests guide regulation. The CRAs reliance on the HES framework prompts an examination of the following contemporary theories on institutionally driven regulation.

One such perspective, the 'systems' theory of regulation is built upon the premise of a systemic inability of clear communication among various actors in a system. A regulator may directly influence the market through law, but without a clear translation of regulatory parameters into market parameters, said influence will still be responded to in adherence to market norms, thereby putting the market and regulators either at odds with, or indifferent to one another.[33] This theory instead places regulators at a position of indirect influence, using regulation as a way to essentially 'proceduralise' market activity towards a desirable direction instead of directly prescribing how market/s must act through sanction-backed legislation, thereby bridging inter-institutional communication gaps.[34]

The CRAs approach to PDE cybersecurity prescribes essential cybersecurity requirements for market entry,[35] allowing market operators to 'opt for' HESs[36] as a concrete way to demonstrate conformity. One could claim that the CRA thus 'proceduralises' product cybersecurity, using

---

[30] Jacobides & Ors. 2018 (N28), at 2256

[31] *Jacobides & Ors. 2018* (N28)*, 2256-57,* ecosystems have been classified into broad groups: Business, innovation and platform

[32] Eliantonio, M., & Medzmariashvili, M., Hybridity under Scrutiny: How European Standardization shakes the foundations of EU Constitutional and Internal Market Law, (2017) Legal Issues of Economic Integration 44:4, 323-36 (Eliantonio & Anr. 2017); Scott, C., Regulation in the age of Governance: The Rise of the Post-Regulatory State, in Jordana, J., Levi-Faur, D. (eds.), The Politics of Regulation, (2004) Edward Elgar, 145-176 (Scott 2004); Yeung, K., Ranchordas, S., *An introduction to law and regulation: Text and Materials,* 2nd Edition, (2024) Cambridge University Press, Chapter 4 (Yeung & Ranchordas 2024), available at https://www.cambridge.org/core/books/an-introduction-to-law-and-regulation/theories-of-regulation/9D5591DBE482C5922D5F001F062C0531, at 120, 137

[33] Scott 2004 (N 32), 152-53

[34] *Ibid,* 154

[35] Cyber Resilience Act (N15), Annex I

[36] Cyber Resilience Act (N15), Article 27 & Article 32(2)

ascertained market entry and user trust (through the CE marking)[37] as incentives to conform. This claim comes under question once HESs supporting the CRA are more deeply examined.

Systems theory characterises institutional interactions as linear. Institutional relationships, in this case among regulators and market operators, is still seen as unilateral, the key element being a more modest understanding of regulators' legal capabilities, relegating them to exerting only indirect influence.[38] If visualised based on this conceptualisation, a simplistic view of institutional interactions in EU product cybersecurity would look something like this:

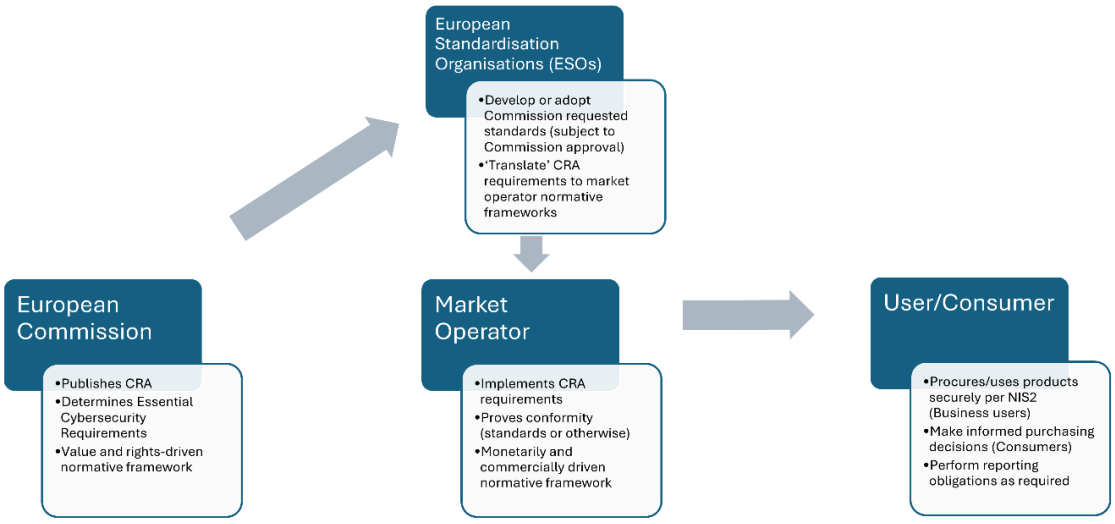

Figure 1: An overview of the CRA regulatory framework based on systems theory

The CRAs regulatory approach, however, is more nuanced. A technical standard being independently developed in response to CRA requirements may be reflective of systems theory. However, HESs are not exactly developed 'independently' through mere indirect influence. The Commission initiates (through standardisation requests) and decides on the adoption of HESs supporting the CRA, further exerting indirect control through financing.[39] Referral in the Official Journal of the European Union[40] brings with it more factors of external influence by rendering these HESs subject to constitutional and governance concerns mentioned earlier in this article (Section 1.2). Standards development may account for industry-driven interests, since ESOs are required to attain consensus from their members[41] (which include market operators), the PDE performance metrics and specification requirements that guide these HESs are determined by the Commission through legislation and policy.[42] This gives the regulator –

[37] Cyber Resilience Act (N5), Recitals 36, 89, r/w Article 3(31), Article 29 and Article 30, Regulation (EC) No. 765/2008, Article 30
[38] Yeung & Ranchordas 2024 (N32), 139
[39] Standardisation Regulation (N9), Article 15
[40] Standardization Regulation (N9), Article 10(6)
[41] Standardisation Regulation (N9), Article 10
[42] Standardization Regulation (N19), Article 10(1); Cyber Resilience Act (N15), Annex I; Commission Implementing Decision on a standardization request in support of Regulation (EU) 2024/2847, C (2025) 618

the Commission - significant direct influence over how the market may act under its own normative framework.

This reflects an inter-institutional interaction that is multilateral, involving activity that does not merely guide normative frameworks of institutions involved, instead combining their capacities and employing them to further regulatory objectives. Combining these normative frameworks allows for multilateral, continuous and clearer communication (and therefore influence) among institutions, while also providing concrete avenues for such communication through legal mechanisms.[43] Characterising CRA-led HESs as avenues of translating and proceduralising the Commissions otherwise unilateral regulatory influence would thus reflect an incomplete view.

2.2 Applying networked theories of regulation to PDE cybersecurity – an examination

One might also consider the possibility of using 'networked' theories on regulation. These theories look at multilateral relationships between actors as reflecting either collaboration or intermediation.[44] Notwithstanding the kind of relationship, there is a clear regulator and a clear 'regulatee.' Regulatory responsibility is either shared by or mediated through non-state actors, which are usually private or administrative bodies that operate in pursuance of regulator-prescribed obligations, but with varying degrees of discretion/autonomy.[45] Networked theories account for, to a higher degree than systems theory, multilateral and continuous communication between actors in a market. However, applying them to the CRA and the HES framework brings up some incongruencies.

Networked theories conceptualize regulation as a 'regulatory chain', with a unidirectional flow of influence (Regulator – Mediator/collaborator – Regulatee).[46] While there could be some overlaps between collaborators and regulatees, rule-making power itself vests yet with a specified regulator.[47] When, alternatively, actors are perceived as intermediaries, their role is considered akin to a principal-agent model.[48] The nature of an intermediary, nature of shared authority, incentives to intermediate and the interests intermediation serves, reasons for intermediation, are all assumed to be fluid.[49] While fluidity allows for interpretative openness, it still is premised upon a unilateral flow of rule-making and market intervention authority. A

---

final (CRA Standardisation request), available at https://ec.europa.eu/transparency/documents-register/detail?ref=C(2025)618&lang=en, Annex II

[43] Standardisation Regulation (N9), Article 5, Article 7, Article 10(2)-(5), Article 12

[44] van Erp, J., Wallenburg, I., Bal, R., *Performance Regulation in a Networked Healthcare System: From Cosmetic to Institutionalized Compliance,* (2020) Public Administration 98(1) (van Erp & Ors 2020); Abbott, K.W., Levi Faur, D., and Snidal, D., *Theorizing Regulatory Intermediaries: The RIT Model,* (2017) The Annals of the American Academy of Political and Social Science 670(1) (Abbott & Ors. 2017); Yeung & Ranchordas 2024 (N32), 140-41

[45] Van Erp & Ors 2020 (N44), at 48; Abbott & Ors. 2017 (N44) at 15

[46] Abbott & Ors. 2017 (N44), at 17;

[47] Van Erp & Ors (2020) (N44), Section 5; Maggetti, M., Networked Regulation: The European Experience, in Introduction to Regulation and Governance, (2025) Edward Elgar Publishing (Maggetti 2025), https://doi.org/10.4337/9781035302840.00007, 54-61; Hennessy, O., Mugge, D., European Standardization in flux: Navigating delegation and control in AI governance, (2026) TU Delft Open Publishing (Hennessy & Mugge 2026), https://doi.org/10.59490/jos.2026.8346, 4-6

[48] Abbott & Ors. 2017(N44), 17

[49] *Ibid,* 19-21

networked view of European product cybersecurity regulation would look like the diagram hereinbelow.

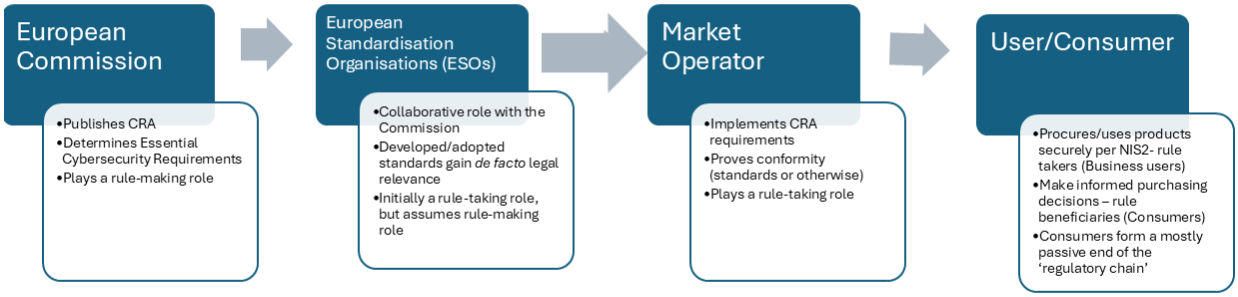

Figure 2: The CRA Cybersecurity Landscape seen through a networked lens

However, the HES framework employed for PDE cybersecurity in anything but unilateral, deviating quite significantly from a 'regulatory chain.' HESs, while providing an avenue to 'translate' the normative framework of regulators (e.g., public values, rights, safeguards, etc.) into the normative framework of regulatees (e.g., technical requirements, product design, etc.) also allow ESOs significant interpretative liberty thereby allowing said interpretations to directly impact normative frameworks that inform regulator actions.[50]

This interpretative liberty, coupled with ESO membership structure-enabled market operator representation provide a stark contrast to the unilateral regulatory approach envisioned by systems-based and networked-based theories. Therefore, a holistic theoretical approach must perceive actors in the PDE cybersecurity space not just in defined roles of rule-makers and rule-takers but also accounts for the inherent dynamism of market actor roles characteristic of standardization in pursuits of EU product cybersecurity.

Conventional institutional theories may be amenable, yet sub-optimal to examine PDE cybersecurity standardisation. This section identified two elements that cause this insufficiency. A comprehensive theoretical understanding must thus account for these elements. Firstly, it must account for dynamism between rulemaking and rule-taking roles of actors. Secondly, it must also account for a possible plurality of actors in whom rule-making power is vested, *de facto* or *de jure.* This is where the theory of ecosystems may prove useful.

Section 3: Building the European Product Cybersecurity ecosystem

[50] Kamara, I., *European cybersecurity standardization: a tale of two solitudes in view of Europe's cyber resilience,* (2024) Innovation: The European Journal of Social Science Research 37:5 (Kamara 2024), available at https://doi.org/10.1080/13511610.2024.2349626, 1446; Commission, *An EU Strategy on Standardisation,* COM(2022) 31 final (EU Standardisation Strategy 2022), available at https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52022DC0031, 4

The first aspect to consider is what an 'ecosystem' would mean in a regulatory context. The term itself has seen significant evolution in usage over time; this article builds on its interpretation in a strategy and business context.[51]

A strategy lens on ecosystems – their formation and characteristics, would reveal that when variability of actors and the relationships among them are abstracted into where value lies and where said value is monetised, just operating in the market is premised upon factors other than presence of a product/service to sell; prevalent rules, roles of other actors, ability and limits to monetization, all affect decision making.[52] This plurality of factors necessitates the use of an ecosystem perspective to understand a market clearly.

In that respect, the definition suggested by Jacobides and Ors. i.e., '*An ecosystem is* ***a set of actors*** *with varying degrees of* ***multilateral, nongeneric complementarities*** *that are* ***not fully hierarchically controlled****,'* (emphasis added) may be tested against the European product cybersecurity landscape to determine its applicability. This section applies this definition to European PDE Cybersecurity, clarifying actor roles, the specific role ESOs have in the HES framework, and identifying complementarities arising from this framework that incentivise market actors with otherwise diverse interests to align their activities around the framework.

3.1 Analysing actors:

The earlier analysis on institutional perspectives has already provided a basic idea on relevant actors involved. The primary public rulemaking (or "State") role is assumed by the European Commission. The Commission, based on the mandate provided to it by the Treaty on the Functioning of the European Union (TFEU),[53] prescribes essential cybersecurity requirements through the CRA. The Commission may also specify European Cybersecurity Certification Schemes (ECCSs) adopted per the Cybersecurity Act that may be used to demonstrate conformity with CRA requirements, with certifications of assurance level 'substantial' or higher eliminating the need for third-party PDE conformity assessment regardless of its risk classification.[54]

HESs supporting the CRA can be used by a wide range of PDEs – those not classified as 'critical' or 'important' in Class II - to demonstrate conformity.[55] HESs thus assume an integral role in enabling harmonised PDE cybersecurity. The HES framework allows standards developed under the CRA Standardisation request to preclude any existing standards in Member States.[56] Developed HESs must also not only be reflective of EU policy but must also be market friendly.[57] Market effects of harmonised standards are also an important consideration; costs associated with employing alternative means of conformity

[51] Jacobides & Ors. 2018 (N28), Section 2
[52] Jacobides & Ors. 2018 (N28), 2265-66
[53] Treaty on the Functioning of the European Union, Article 114
[54] Cyber Resilience Act (N15), Article 27(8)-(9) r/w Regulation (EU) 2019/881 on ENISA and on information and communications technology cybersecurity certification OJ L 151/15 (EU Cybersecurity Act), Article 52(6)-(7)
[55] Cyber Resilience Act (N15), Article 27(1), Article 32(2)
[56] Standardisation regulation (N9), Recital 14; Cassis Dijon (N6)
[57] Standardisation Regulation (N9), Article 10(1)

demonstration[58] additionally afford a kind of 'derived normativity'[59] to the outputs of private rulemaking by ESOs.

Conventionally, forms of private regulation such as standards have been considered resulting from absence of State action or post the consequences of State mismanagement.[60] However, the CRA affords ESOs *de facto* rule-making roles proactively, by leveraging a nascent market (PDE cybersecurity) to achieve global innovative competitiveness as well as pursuing objectives characteristic to State normative frameworks such as public health and safety. This obscures the role of ESOs in product cybersecurity, making their distinction as an agent of the State or a peer of the State difficult to crystallise. Said crystallisation would require a deeper understanding European standardisation as a process, done further along in section 3.2.

The next actor examined is the European Agency for Network and Information Security (ENISA). Formed in 2004, it received a revised mandate through the Cybersecurity Act.[61] ENISAs mandate includes support and collaborative work (including preparing Commission-requested certification schemes) assigned to it through the Cybersecurity Act and any other Union legislation such as the CRA.[62] Under the CRA, ENISA is tasked with assistance towards Member State cybersecurity capacity building, coordinating vulnerability reporting across relevant actors and institutions at the Union and national level, epistemic and technical support, and market surveillance activities coordination.[63] ENISA therefore emerges as an actor with epistemic expertise that assumes primarily a coordinative and supportive role, beholden to tasks enabled through specific legislation. ENISA may thus be seen as an administrative body or a regulatory agent, since it has no rule-making power, but plays a part in rule-enforcement and procedural assistance across pretty much every level of the European cybersecurity landscape.

The next set of actors to consider is market operators. *Prima facie,* market operators assume primarily a rule-taking role is viewed solely under the CRA. Regardless of what position a market operator may occupy in a PDEs supply chain, CRA cybersecurity and other obligations apply at the point of placement of a PDE on the market.[64] In the overall cybersecurity landscape, however, CRA-prescribed market operator activities are wider than just PDE conformity. Obligations regarding reporting and coordination with national Computer Security Incident Response Teams (CSIRTs) and ENISA bolster institutional activities in furtherance of the NIS2 Directive and the Cybersecurity Act.[65] Market operators also contribute to CRA-driven standardisation activities by participating in the process of developing harmonised

---

[58] Schepel 2013 (N7), 527-28
[59] Delimatsis 2023(N23), 573
[60] *Ibid,* 571-73
[61] EU Cybersecurity Act (N54), Title II
[62] Markopolou, D., Papakonstantinou, V., & de Hert, P., The new EU cybersecurity framework: The NIS Directive, ENISA's role and the General Data Protection Regulation, (2019) Computer Law & Security Review 35 105336, https://doi.org/10.1016/j.clsr.2019.06.007 (Markopolou *et al* 2019), at 8; EU Cybersecurity Act (N54), Title II, Chapters I and II
[63] Cyber Resilience Act (N15), Articles 10, 14-16, 33 and Chapter IV
[64] Cyber Resilience Act (N15), Article 1(a)-(c), Articles 13-15, 18-22, 24, 28-32,
[65] Cyber Resilience Act (N15), Article 14; NIS2 Directive (N15), Article 11(4); EU Cybersecurity Act (N54), Article 7/Chapter II

standards indirectly as members of NSOs and directly as members of ETSI.[66] Attributing a mere rule-taking role to market operators would therefore be an incomplete view. The extent of their rule-making role is explored in detail further in Section 4.2 after employing an ecosystems-based perspective.

The final set of actors is the user/consumer, natural or legal entities that employ PDEs. They may be considered primarily as beneficiaries of outcomes produced by other actors performing their obligations under the CRA. While they may play a voluntary role in enhancing PDE cybersecurity through vulnerability reporting and coordination with other actors, they are in no way obligated by the CRA to so act. Establishing a more resilient digital market may be said to promote a distal outcome in enhancing user and consumer resilience and safety without specifically affording them with additional rights or duties; a distal outcome not unfamiliar to product harmonisation legislations in general.[67]

3.2 Examining ESOs:

The previous subsection telegraphed the need for a deeper look into the role played by ESOs in European product cybersecurity. Harmonised standards are viewed as an efficient and market-friendly avenue to tangibly operationalise legislation on (digital) products in the market. The CRA projects a similar characterisation in a PDE context as well. However, while ESO deliverables are essentially voluntary in nature, their formal recognition in law and market effects of said non/compliance bestow upon them significance much higher that what their voluntary nature may initially suggest.[68] Thus, viewing ESOs purely from the CRA lens would be incomplete.

Established to assist with standards development at the request of the Commission, ESOs form an important element of product regulation at the Union level. ESOs essentially, are private nonprofits, carrying standardisation work not just in response to EU law but also through stakeholder initiative. EU legislation driven standards development, such as under the CRA, form a minor portion of the standardisation work undertaken by ESOs.[69] However, their membership models differ, with CEN and CENELEC being conglomerations of relevant NSOs representing stakeholder interests, while ETSI allows direct economic operator membership.[70] However, when it comes to harmonised standards, such as those developed pursuant to the CRA standardisation request, decisions regarding acceptance of standardisation requests,

---

[66] Cyber Resilience Act (N15), Chapter 3; Standardisation Regulation (N9), Articles 5 & 13
[67] Chiara, P.G., Towards a right to cybersecurity in EU law? The challenges ahead, (2024) Computer Law and Security Review 54 105961, https://doi.org/10.1016/j.clsr.2024.105961 (Chiara 2024), Section 3
[68] Senden, L., Towards a more holistic legitimacy approach to Technical Standardisation in the EU, in Eliantonio, M. & Cauffman, C. (eds.), The Legitimacy of Standardisation as a Regulatory Technique, (2020) Edward Elgar Publishing, https://doi.org/10.4337/9781789902952.00007 (Senden 2020), Chapter 2, at 24; Werle, R. & Iversen, E., 'Promoting Legitimacy in Technical Standardisation,' (2006) Science, Technology & Innovation Studies Vol. 2, https://scispace.com/pdf/promoting-legitimacy-in-technical-standardization-1dc1ppxyya.pdf (Werle & Iversen 2006), pp. 21-23
[69] A majority of proposals for European standards come from stakeholders through NSOs; https://www.cencenelec.eu/european-standardization/european-standards/
[70] Delimatsis 2026 (N29), 37-8

acceptance of new work items, and on adoption, revision and withdrawal of standards may only be made by NSO representatives within those ESOs.[71]

Organising European standardisation based on direct and indirect participation (through notified National Standardisation Organisations or "NSOs") of all relevant stakeholders does allow for epistemic expertise being available during standards development.[72] Requests for standards are additionally required to take into account stakeholder interests - often represented via stakeholder organisations - and have consensus. Such representation for other stakeholders such as consumer and environmental organisations through the Standardisation Regulation, is a reason why the regulation has been characterised as constitutionalising European standardisation to a significant degree.[73] Prof. Delimatsis, in a discussion paper from 2025, provides a comprehensive diagrammatic overview of the relationships between ESOs, the Commission, economic operators, and global standardisation efforts, reiterated hereinbelow:[74]

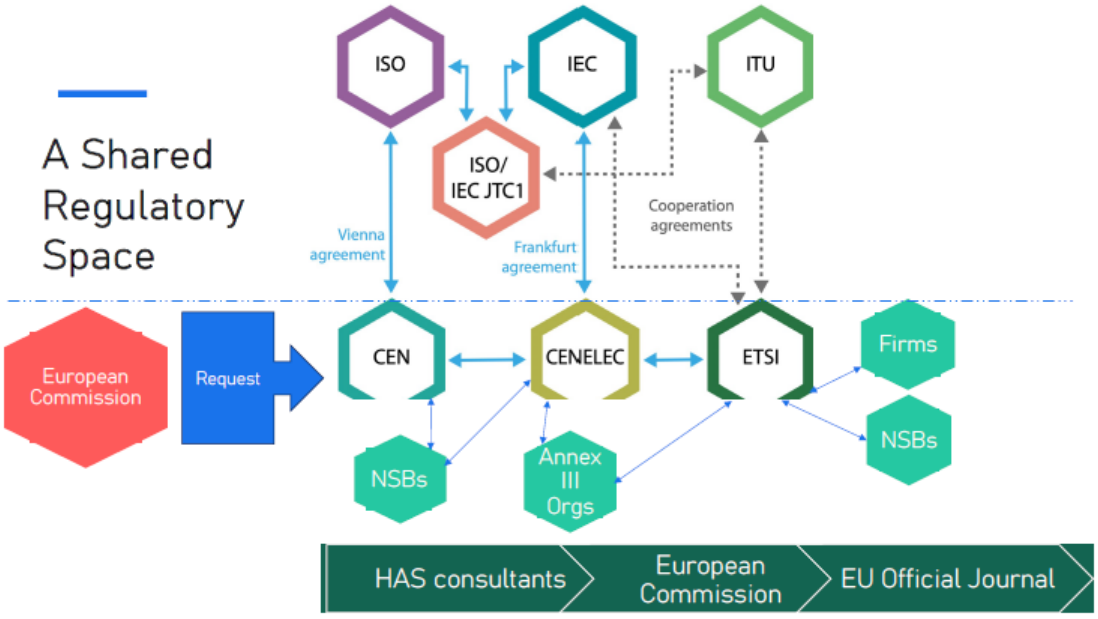

Figure 3: "A shared regulatory space for EU Standardization

CRA-relevant standards were requested from the ESOs by the Commission via an implementing decision in early 2025.[75] The CRAs broad scope demands commensurate conformity assessment avenues, reflected through requests for both broader-scoped horizontal

[71] Regulation (EU) 2022/2480 amending Regulation (EU) No 1025/2012 as regards decisions of European standardisation organisations concerning European standards and European Standardisation Deliverables, OJ L 323/1 (Regulation 2022/2480), Article 2; Delimatsis 2026 (N29), 37-8
[72] Standardisation Regulation (N9), Article 27, Recital 2
[73] Delimatsis 2026 (N29), 38-9
[74] Delimatsis, P., A Shared Regulatory Space for EU Standardization – Origins, Evolution and prospects, (2025) TILEC Discussion Paper DP 2025-09 (Delimatsis 2025), 9
[75] CRA Standardisation Request (N42)

standards and vertical standards for PDEs performing higher-risk functions.[76] Broadly applicable horizontal standards such as *inter alia* for secure design and data security and protection principles have been tasked to CEN and Cenelec.[77] Additionally, cybersecurity standards for 'critical' PDEs have also been assigned to them.[78] Cybersecurity standards for 'important' PDEs have been assigned to all three ESOs.[79]

Pursuant to the request, standardisation work is in progress at the time of writing this article. CEN/Cenelecs technical committee on cybersecurity and data protection, the Joint Technical Committee 13 (hereinafter, "JTC13") has two working groups currently working on CRA-related standards.[80] These JTCs also have significant representation from economic operators, as they are the primary source for epistemic expertise. ETSI recently made available draft versions of standards being developed for 'important' PDEs.[81] ETSI has also opened informal public consultations for the draft standards, allowing stakeholders to comment on available drafts that may or may not be implemented based on concreteness of contributions within them.[82]

Based on the CRA-specific standardisation process, and a general understanding of European technical standardisation, a CRA-specific modified diagrammatic representation of the role of ESOs based on the representation in Figure 3 above may be made. Such a diagrammatic view outlines the intersection between economic operators in cybersecurity and NSOs, further outlining their multifaceted role. Economic operator contribution to ESO standardisation work is more directly visible in the development of standards, and more indirectly visible through their representation in NSOs, and in stakeholder organisations (through small and medium enterprises).[83] Clarifying this intersection and role allows for an informed examination of complementarities cementing the formation of a PDE cybersecurity ecosystem in Europe. A CRA-specific diagrammatic overview is hereinbelow:

---

[76] *Ibid*, Annex I,
[77] CRA Standardisation Request (N42), Article 1(2) r/w Annex I, Points 1 to 15
[78] CRA Standardisation Request (N42), Article 1(2), r/w Annex I, Points 39 to 41; Cyber Resilience Act (N15), Annex IV
[79] CRA Standardisation Request (N42), Article 1(2) r/w Annex I, Points 16-38; Cyber Resilience Act (N15), Annex III
[80] JTC13 Working Group 6 is currently working on critical PDEs and a standardized process for sectoral cybersecurity risk assessments based on EN 18037, and Working Group 9 is working on horizontal cybersecurity standards based on cybersecurity requirements for all PDEs; https://www.stan4cra.eu/cenclcjtc13
[81] Examples include Draft ETSI EN 304 623 V0.1.3 (June 2026), available at https://www.etsi.org/deliver/etsi_en/304600_304699/304623/00.01.03_20/en_304623v000103ev.pdf; other standardisation deliverables at the 'draft' and 'mature draft' stages may be found at https://docbox.etsi.org/CYBER/EUSR/Open
[82] ETSI, How to comment on draft standards, 17/04/2026, https://docbox.etsi.org/CYBER/EUSR/Open/ETSI_CYBER-EUSR_Commenting_instructions_open%20consultations_17-04-2026.pdf
[83] Standardisation Regulation (N9), Annex III

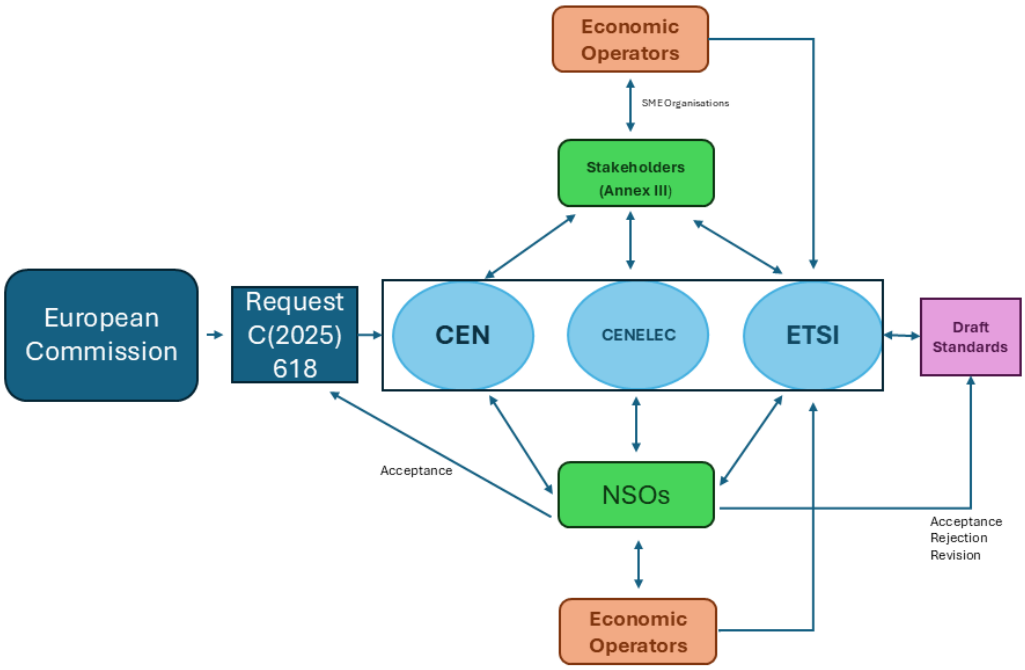

Figure 4: A CRA specific overview of ESO roles in PDE cybersecurity standardisation. Arrows represent direction of influence

3.3 Clarifying Complementarities:

Now, a contextual disambiguation of inter-actor complementarities may commence. Complementarities may exist in markets characterised by role/expertise-based modularity within actors, requiring actor coordination that cannot be solely market or regulator driven.[84] Foundationally, they may take different forms depending on the degree of interdependence among actors and degree of value derived from said interactions.[85] However, it has been posited that for an ecosystem to form, there must be unique (one cannot function without the other) or super-modular (value addition to one adds value to the other) complementarities that are nongeneric, creating value wherefrom would require interaction-specific structural relationships.[86]

When viewed from a CRA-led HES lens, it is possible to distil form(s) of complementarities that emerge. The Standardisation Regulation acknowledges the value technical standards provide in fostering a digital single market through reduced Member State fragmentation that directly contributes to easier purchasing decisions for users and consumers.[87] PDE cybersecurity legislation bolstered through CRA-driven standards may (validly) be dubbed as a 'co-regulatory' approach wherein economic operators directly contribute their epistemic expertise in the rule-making process, bolstering otherwise high-level product requirements through "formally non-binding, yet legally salient" cybersecurity standards.[88] Reliance on

[84] Jacobides & Ors. 2018 (N28), 2256, 2260
[85] A detailed description of the types of ecosystems is provided in Jacobides & Ors., 2018 (N28), at 2261-63
[86] Jacobides & Ors., 2018 (N28) at 2263
[87] Kanevskaia 2020 (N3), at 62
[88] Kanevskaia 2020 (N3), 63-65; Teichmann, F., & Sergi, B.S., The EU Cyber Resilience Act: Hybrid Governance, compliance and cybersecurity regulation in the digital ecosystem, (2025) Computer Law &

technical specifications in the absence of available standards signals even more strongly of the indispensable and augmentative value epistemic expertise of economic operators provides to PDE cybersecurity requirements promulgated within the CRA.[89] Thus, CRA-driven standardisation may be seen as a clear instance of complementarity between the Commission and economic operators, one managed by ESOs and NSOs through procedures established in the Standardisation Regulation. The presence of such a specific structure of alignment between various actors to allow industry expertise while also maintaining European values clearly establishes this complementarity as nongeneric.[90]

High-level CRA requirements can be met through avenues other than harmonised standards or technical specifications. However, recourse to harmonised standards reduces Member State fragmentation,[91] bolsters the single market for PDE cybersecurity, involves stakeholder and epistemic inputs in the rule-making process,[92] all while ensuring accountability through judicial review.[93] This is a clear indicator of this complementarity being super-modular in nature, and not unique.[94] PDE cybersecurity law can technically function without dedicated standards, but value addition in harmonised standards significantly adds value to the law. Therefore, one nongeneric, super-modular complementarity is established, strengthening the proposition to view EU PDE cybersecurity from an ecosystem lens.

PDE cybersecurity standardisation following a relatively 'constitutionalised' process under the Standardisation Regulation, one characterised by transparency, accessibility, and inclusion,[95] lends further credence to an ecosystems-based view by pointing to one more complementarity. Representation of stakeholder organisations enables consideration of issues faced by small and medium-size enterprises (SMEs), consumers, civil society, and environmental issues[96] during standards development. SME contribution to the process of developing harmonised standards being legally recognised and mandated[97] would, at least *prima facie*, guide PDE cybersecurity standardisation in a more equitable direction for economic operators; representation and harmonisation quelling to a certain degree competitive concerns that have accompanied comparable standardisation activity including pre-Standardisation Regulation standardisation in the EU.[98] Harmonised standards being susceptible to judicial review lends them added legitimacy not otherwise afforded to standardisation activity conducted outside the harmonised standards aegis, even if such legitimacy is not sans associated problems.[99] These are some non-exhaustive factors leading to the development of another nongeneric super-modular

---

Security review 59 106209 (Teichmann & Sergi 2025), https://doi.org/10.1016/j.clsr.2025.106209, 4; Case C-613/14, James Elliott Construction Ltd v. Irish Asphalt Ltd. (N10)

[89] Cyber Resilience Act (N15), Article 32

[90] Jacobides & Ors. 2018 (N28), 2261-63

[91] A criticism often levied towards the predecessor of the Standardisation Regulation, the 'New Approach' Directives of 1985; Kanevskaia 2020 (N3), pp. 63-65;

[92] Delimatsis 2026 (N29), p.37-9

[93] Teichmann & Sergi 2025 (N88), 4

[94] Jacobides & Ors. 2018 (N28), 2261-63

[95] Delimatsis 2025, (N74), p.8

[96] Standardisation Regulation (N9), Annex III

[97] Standardisation Regulation (N9), Article 10(1)

[98] Kanevskaia 2020 (N3), pp.78-82

[99] Schepel 2013 (N7)

complementarity – they stem exclusively from harmonised standardisation activity being structured the way it is, and PDE cybersecurity standardisation based on the CRA standardisation request adds immense value to SME operations, and to stakeholder organisations by enabling enhanced representation and oversight.

Building upon the arguments adduced in Section 2 for the relative appropriateness of an ecosystems-based perspective on PDE cybersecurity standardisation, this section was aimed at providing the building blocks for such a perspective. This pursuit led to a disambiguation of actor roles, an understanding of ESOs as the lynchpin for building complementarities, and an understanding of (some) complementarities; these cumulatively enable an ecosystems-based view. The following section introduces the ecosystem of PDE cybersecurity standardisation and explores prevalent discussions in standardisation research through this newly created lens.

Section 4 – An Ecosystem Materialised: PDE Cybersecurity Standardisations impacts

The previous section clarified actor roles within the space of European PDE cybersecurity, and established complementarities that exist exclusively based on the specific structure within which actors perform these roles. This section materialises the ecosystem in its entirety and examines its operation.

4.1 The PDE Cybersecurity Ecosystem: Structure

Once the grounds for an ecosystem's formation are established, what would this ecosystem look like? The first aspect to consider is the presence of an activity fulcrum or core; as Jacobides *et al* describe it, a 'hub.'

A contemporary view from business and strategy perspectives suggest that analyses of existing ecosystems often presume an existing 'central' or 'hub' actor around which said ecosystem is formed and operates, advocating instead for analysis of roles agreed upon by actors through the structure of their alignment.[100] If an alignment of otherwise autonomous actors is to be viewed through their points of intersection, a 'hub' may be seen as the actor that creates circumstances leading to these intersections, while actor coordination can still occur without a central authority structure. A market illustration envisages a focal actor that controls a factor or product from which upstream and downstream actors in that sector derive their products value, compelling them to align around this focal actor (e.g., Android OS being a product around which smartphone manufacturers must align, as should developers that intend to build application for such smartphones.)[101]

To apply this reasoning to PDE cybersecurity regulation, a translation of this concept into a regulatory context is needed. European standardisation has evolved from a need for market-wide equivalence in technical implementation of public policy objectives that the Commission pursues, which is why in translating this concept, inspiration may be drawn once more from the idea of viewing EU standardisation as a shared regulatory space. Harmonised standards

[100] Jacobides & Ors. 2018 (N28), Section 2.2
[101] Jacobides & Ors. 2018 (N28), 2260; Baldwin & Ors. 2024

based on EU law emerge as outcomes of a regulatory space consisting of actors with diverse interests – value-based, technological, commercial, or social – exerting varying degrees of regulatory influence within a structure that tries to optimally streamline these interests.[102]

PDE cybersecurity standardisation specifically, sees ESOs tasked with building standards that guarantee implementation of essential performance metrics prescribed by the Commission in a manner that is technically pragmatic, keeps with principles of good governance, and is amenable to civil society interests. Absence of or inadequacy in any of these elements would jeopardise the approval of proposed harmonised standards. However, one must not infer from this an equivalence among actors pursuing each of these elements. One must instead identify the actors controlling elements necessitating actor alignment.

The first element is the essential performance requirements that PDEs must meet, specified within the CRA Annexes. Standards for PDE cybersecurity have been requested specifically to provide a recognised avenue to meet these requirements. Thus, the Commission plays a pivotal role as the actor that prescribes these requirements. The technical thresholds to meet these requirements, regardless of nature or designer, would be designed around the Commissions prescriptions. This observation is reinforced when one considers that harmonised standards currently under development do not only follow CRA Annex I performance requirements but are built upon Commission provided technical interpretations of important and critical PDE functions.[103]

In addition to this prescriptive role, it is also the primary driver for actor alignment. It mandates the development and controls the adoption of developed standards.[104] Actor alignment is additionally also a result of complementarities characteristic of the harmonised standards development process and of the relative benefits of designing products per harmonised standards as opposed to other standards (discussed earlier in Section 3.3). Therefore, appropriate exercise of the Commissions role would result in a need for other actors in the space to align towards a common end, through to serve uncommon interests. In that regard, the Commission acts as a 'hub' in PDE cybersecurity rendition of the theory of ecosystems. However, this article submits that the Commission is not the only 'hub.'

The Commissions prescriptions inform standards development; the actual logistics of standards development are an ESO function. These logistics include acquisition of epistemic expertise, consideration for civil society stakeholders, and an openness to rule of law principles such as accessibility and judicial review.[105] Acquisition of epistemic expertise is achieved through their membership structures; industry expertise informs standards development indirectly through NSOs in CEN and Cenelec, and directly in ETSI. Representation for and consideration of civil

---

[102] Delimatsis 2025 (N74), 5, 10-11

[103] Commission Implementing Regulation (EU) 2025/2392 on the technical description of the categories of important and critical products with digital elements pursuant to Regulation (EU) 2024/2847, OJ L 2392; For instance, draft ETSI standards developed for 'important' PDEs are built upon these technical descriptions.

[104] Delimatsis, P., Verghese, Z., "To Antipolis, my sisters!": ETSI as a forum of contestation, collaboration and orchestration, (2024) Innovation: The European Journal for Social Science Research 37:5 (Delimatsis & Verghese 2024), https://doi.org/10.1080/13511610.2024.2379806, 1310

[105] Case C-588/21P, Public.Resource.Org and Right to Know v Commission; Case C-613/14, James Elliott Construction Ltd v Irish Asphalt Ltd (N10)

society stakeholders is visible through ESO membership structures. Additionally, such mandated consideration more deeply embeds developed standards into the ecosystem they inhabit – alignment enhances impact.[106] The specific relationships created between ESOs and other actors through Standardisation Regulation mechanisms necessitates other actors to align around harmonised standards, rendering ESOs as 'hubs' as well. Moreover, both the Commission and ESOs, while producing output essential to actor alignment, do not mandate actor alignment. It is the structure of the European standardisation framework that incentivises actor alignment towards their output, another key characteristic of an ecosystem.[107]

In that vein, economic operators while contributing to standards development, would not assume a 'hub' role in this rendering. Firstly, while they do exert influence in ESOs, influence exerted by a specific economic operator depends on several factors, such as the ESOs membership structure, the size of the firm itself, presence in stakeholder organisations, and the amount of epistemic expertise it can offer. Applying ecosystems-theory based understanding, an economic operator may be seen as aligning around the hubs rather than attempting to assume the role of one for two reasons. Firstly, the relative benefits of being involved in harmonised standards development may be seen as incentivising their provision of epistemic expertise. While expertise may also imply influence, that aspect of epistemic influence is discussed later in this section (Section 4.2). Similar reasoning would incentivise alignment from stakeholder organisations as well; representation and legally mandated consideration to their interests strongly encourages alignment with 'hub' outputs. Therefrom, an ecosystems theory view of EU PDE cybersecurity may be constructed as hereinbelow:

[106] Wiegmann, P.M., de Vries, H. J., & Eom, D., Project report: Measuring societal impact of standards, (2023) Technische Universiteit Eindhoven (Wiegmann & Ors. 2023), https://research.tue.nl/en/publications/1e1188fc-352b-4a4c-9cc7-e4dd91f4e579, 100-101
[107] *Supra* Note 90

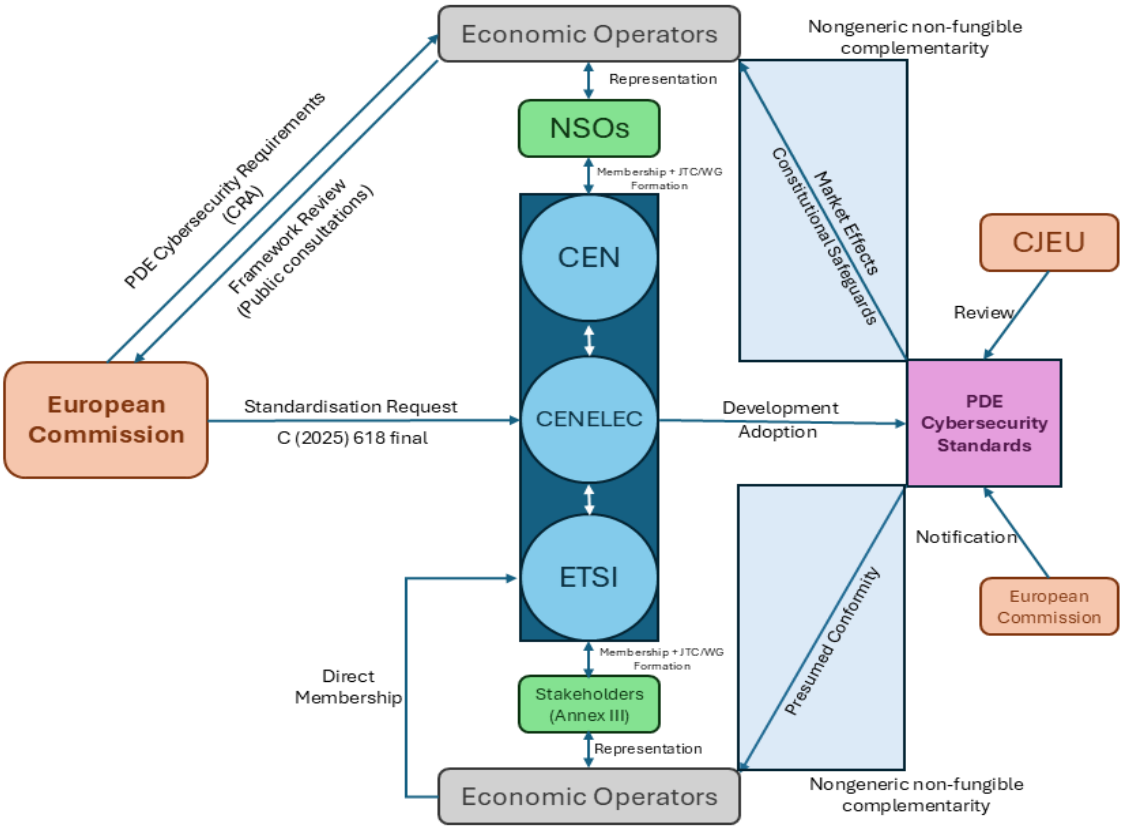

Figure 5: A fully materialised ecosystem for European PDE cybersecurity. Arrows represent direction of influence

4.2 An Ecosystem in Action: The dance of integrated actions and diverging interests

This subsection explores in depth actor interactions within the newly constructed ecosystem of PDE cybersecurity. Complementarities exclusive to the standardisation framework align action towards standards development, but aligned actions still serve divergent interests – alignment is not integration.[108]

Even 'hub' actors, while contributing most of the impetus that drives development do not exhibit a relationship akin to 'integration;' developing harmonised standards is but a minor portion of the work ESOs do.[109] Diverging interests prevent seamless alignment, often resulting in interactions that are not necessarily "collaborative."[110] Literature on private rulemaking and standardisation offers important perspective into these seamed interactions. Aligned actions may be a function of public co-optation in an environment where the public actor (the Commission) and private actors (ESOs) share a competitive dynamic.[111] They may also be seen as a resilience strategy employed by ESOs to maintain external and/or internal legitimacy in

[108] Jacobides & Ors. 2018 (N28), 2263
[109] *Supra* Note 80
[110] Delimatsis & Verghese 2024 (N104), 1310-12
[111] Partiti, E., Bijlmakers, S., & Delimatsis, P., Evolutionary Dynamics of transnational private regulation, (2022) Transnational Legal Theory 13:4 (Partiti & Ors. 2022), https://doi.org/10.1080/20414005.2023.2178143, pp. 435-38

the face of crises.[112] These perspectives position themselves within discussions on power and legitimacy dynamics among public and private rule-making authorities, with thorough sectoral application providing actualisation.[113] They perceive the Commission and ESOs (as a whole) as two distinct and whole actors; determinations on their interactions concerning governance and sectoral matters also thusly informed. An exploration of their specific alignment in PDE cybersecurity, however, would benefit from a more dermal approach.

The Commission determines the breadth, conformity, and final validity of harmonised standardisation activity, but it has no control over its development process or delivered content.[114] The Commission's request for horizontal and vertical standards supporting the CRA confers to ESOs a mandate of immense breadth, meaning that these standards will not only specify how a PDE may perform its specific function securely, but will also represent a normative understanding of what a secure PDE means.[115] A normative determination would informs the perception of a secure PDE among the Commission and market operators, but directly impacts consumer and societal expectations from and interest in a secure PDE. With the content of this normative understanding completely within ESO purview, it is valuable to consider intra-ESO coordination as well.[116]

An ecosystems-based perspective assists in this endeavour without isolating it from pressing external and normative concerns. Concerns about private rule-making, especially in product markets, are often underpinned by a perceived desire among economic operators to pre-empt, prevent, or even inform the exercise of rule-making authority by a public actor, often in the wake of a breakdown of a sectors organisational framework.[117] One may argue that structuring private rule-making for PDE cybersecurity around the harmonised standards framework significantly quells these concerns, standardisation activity stems from Commission requirements and rather uniquely, have societal and stakeholder representation baked into the process. This would be a strong argument if PDE cybersecurity was a purely sectoral objective. The normative implications of horizontal cybersecurity standards, however, open a novel possibility for ESOs. They may now be able to define the very core of European product cybersecurity's organisational framework, i.e., what a cybersecure PDE even means.

In building this definition, ESOs are only beholden to maintaining internal legitimacy, i.e., preserving the interests of their members. This effectively negates the need for external

---

[112] Delimatsis & Verghese 2024 (N104), Section 3

[113] Examples of sector-specific explorations include Glinski, C. & Rorr, P., Regulating Certification Bodies in the Field of Medical Devices: The PIP Breast Implants Litigation and Beyond, (2019) European Review of Private Law 2-2019, Section 5.3; Renckens, S., Private Governance and Public Authority: Regulating Sustainability in a Global Economy, (2021) Cambridge University Press, https://www.cambridge.org/core/books/private-governance-and-public-authority/85A9399D25F4FB7AAAF937A360D05AB4

[114] Case C-630/16 of 17 December 2017, Anstar Oy v. Turvallisuus-ja kemikaalivirasto (Tukes) (Anstar v Tukes 2017), https://infocuria.curia.europa.eu/tabs/document?source=document&text=&docid=197826&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=2573508, Paragraphs 35-36;

[115] Kamara 2024(N50), 1449

[116] Kamara 2024 (N50), Section 4.1 provides a detailed account of ESO composition and coordination dynamics in developing harmonized standards for the CRA

[117] Delimatsis 2023 (N29), 567-69

legitimacy; that has already been afforded through the framework of Regulation 1025/2012. High innovative velocity and dynamism intrinsic to digital technologies such as PDEs further reduces external legitimacy concerns. The Commission does have a supervisory role, but within a regulatory ecology with high epistemic asymmetry where the keystone concept is defined by ESOs, such supervision may be deferred at best and reluctant at worst.[118] A private rule-maker would not need to wait for the breakdown of an organisational framework (crisis) to climb or free-ride[119] to a position of higher rule-making authority when they themselves determine what the organisational framework looks like.

With ESOs having to maintain internal legitimacy being the sole *de facto* concern, the PDE cybersecurity ecosystem looks conducive to ESO members possessing epistemic expertise to undergo a significant rule-making power-creep. Members with such epistemic expertise mainly comprise of economic operators, thereby providing them with a disproportionately high ability to experience this incremental creep in power. This possibility of a power creep does not come without associated challenges, even though these challenges do not arise from contemporary concerns of institutional legitimacy or crisis resilience.

4.3 A pillar of steel and a pillar of sand – Economic operators and the PDE Cybersecurity Ecosystems reliance on regulatory bodies

An ecosystems view of European PDE cybersecurity demonstrates an ecology where economic operators may be afforded the ability to acquire significant rule-making power as members of ESOs that need maintain primarily internal legitimacy. However, as established in Section 3.1 of this article, their most prominent role is that of a rule-taker; their products must meet CRA requirements, regardless of their contribution to those requirements' materialisation and what form they take.

Harmonised standards form the output of the European PDE Cybersecurity Ecosystem. This output is valuable to market operators as an avenue to demonstrate that their products meet the essential cybersecurity requirements promulgated by the Commission.[120] The CRAs purpose-based risk classification places most PDEs in the 'default' classification. 'Default' PDEs and certain 'important' PDEs that conform with CRA-led harmonised standards benefit from presumed conformity to the CRA.[121] The limited kinds of PDEs specified as 'important' and 'critical' within CRA Annexes show that most PDEs in the European market would therefore benefit from presumed conformity on applying relevant harmonised standards, significantly reducing compliance burdens they would face if alternative conformity avenues were pursued.

The process of developing standards, however, has consistently demonstrated a speed not adequate to meet market needs.[122] This inadequacy has been attributed to procedural, quality and communication gaps, the non-fungible legitimation afforded through their *de facto* status

[118] Delimatsis 2023 (N29), 573
[119] Delimatsis 2023 (N29), 570-73
[120] Cyber Resilience Act (N15), Article 32
[121] Cyber Resilience Act (N15), Article 27
[122] Commission Staff Working Document, Evaluation of Regulation (EU) No 1025/2012 on European Standardisation, SWD (2025) 170 final (Standardisation Regulation Evaluation 2025), 66

as EU law and subsequent openness to judicial review, and the monopolistic role of ESOs as developers of harmonised standards.[123] Applying an ecosystems perspective to these considerations reveals some additional nuance.

SMEs face considerable challenges, procedural and epistemic, in contributing to the standardisation process, hampering their representation. More generally, stakeholder organisations, present to make the process more inclusive, face procedural and structural barriers to their contribution as well.[124] The inability of several stakeholders to effectively contribute suggests an influence dichotomy among ESO members as well. Market operators may benefit from a possible power-creep as explained in the previous sub-section, but the distribution of these benefits may not be equitable. Thus, several market operators, while being able to contribute to PDE cybersecurity standards, may not be able to benefit from this ability. Since standards development requires consensus, inability to contribute would suggest hesitation on agreement as well, a factor that possibly exacerbates developmental inefficiency.

Additionally, important and critical PDEs, while significantly smaller in scope, must demonstrate conformity through avenues that involve assessment by regulatory bodies (notified bodies/NBs) or conformity with relevant European Cybersecurity Certification Schemes developed by ENISA per the EU Cybersecurity Act. These notified bodies must also possess the epistemic capacity to determine whether a product conforms with relevant cybersecurity requirements, a requirement also presumed as met if there exist relevant harmonised standards that are conformed to.[125] Notified body requirements do included safeguards against unfair assessment activities, but those do not preclude the risk of cultural capture by repeated interactions with market operators in assessing their PDEs.[126] This risk may also be exacerbated when one considers the prior aspect of power-creeps being concentrated towards larger market operators among ESO members.

There is another unlikely addition to a possible power-creep in such a manner. This addition points to another systemic issue in the European product regulation framework. This framework has been found to be needing reworks specific to notified bodies; there is a lack of uniformity among them as accreditation is not mandatory, which further makes monitoring them difficult.[127]

Concluding Remarks:

This article was inspired by curiosity about the impacts of increasing regulatory reliance on avenues of private rulemaking such as technical standards, exemplified in the European Union through its ever-evolving standardisation framework. Further inspiration stemmed from the Commission's attempt at regulating a novel regulatory objective – cybersecurity – using

[123] *Ibid,* 66-67
[124] *Ibid,* 67
[125] Cyber Resilience Act (N15), Article 39 & Article 40
[126] Delimatsis 2023 (N29), 572
[127] Commission Staff Working Document, Evaluation of the New Legislative Framework, SWD (2022) 364 final/2, p. 59

mechanisms that are heavily reliant on technical standards. Product cybersecurity under the Cyber Resilience Act garnered intrigue; its requirement for not just sectoral standards, but also horizontal standards applicable to every digitally enabled product significantly augments standards' importance as an avenue to prove legislative conformity. Whether existing perspectives on the impact of standards on the organisational dynamics of markets – balance of regulatory influence among actors, the relational dynamics between public and private rulemaking - would be affected by these developments is the question this article sought to explore.

This endeavour initially required identifying an appropriate theoretical perspective from which to view the landscape of European product cybersecurity regulation. This article finds that contemporary institutional and networked perspectives on regulation do not holistically encompass EU product cybersecurity. An approach that accounts for dynamic interactions between actors and multilateral exertion of rule-making authority and influence would be required, prompting the idea of using the theory of ecosystems in a regulatory context – applying it to product cybersecurity governance.

However, applying a theory primarily applied to business strategy and market-based considerations required establishing some congruencies. Identifying relevant actors and disambiguating their roles was the next step this paper embarked upon. It identified actors active in the product cybersecurity space, and explored in depth their roles, including a deeper dive into ESOs due to their central and multifaceted role as recipients and drivers of rule-making authority. Next this paper identified and explained complementarities that arise from the CRAs use of the framework for Harmonised European Standardisation. These complementarities – arising from a standardisation framework that encompasses market operator interests, stakeholder interests, civil society interests, and policy considerations, all while having constitutional safeguards such as transparency, accessibility and judicial review – are what incentivise independent actors with diverse interests to align their activities to maximise collective value addition.

Finally, this article builds a ecosystems-based view of European product cybersecurity. It explains the ecosystem in text and with a visual rendition. It then examines actor dynamics as they form and attempts to answer the question at the basis of this article – what the impact of the CRAs heavy reliance on harmonised standards on actor dynamics in the product cybersecurity space is. It identifies changes in market dynamics, building upon existing literature on standardisation by demonstrating a significant incremental shift in market operator rule-making ability from a theoretical perspective. It also telegraphs factors that may influence – augmenting or hindering – this increase. While limited due to an absence of notified standards at the time of writing, it builds a theoretical foundation that would allow for easier practical evaluation once standards are developed, notified, and put into practice. It is safe to say that current and future developments in the European product cybersecurity space are rife with potential for academic exploration – an altogether exciting prospect.